REMARKS

This application has been carefully reviewed in view of the above-referenced Office Action in which new grounds for rejection have been presented. Reconsideration is requested in view of the following remarks.

REQUEST FOR INTERVIEW

The undersigned respectfully requests the courtesy of an interview. Such interview was requested by telephone on Feb. 9, 2009, but no response was received. Applicant believes that the issues in this application can be cleared up in such an interview thereby avoiding the necessity of an appeal.

REQUEST FOR COMPLIANT OFFICE ACTION

As noted in the request filed on Feb. 9, 2009, Applicants' representative requested that a new Office Action be sent due to an error appearing in the top of page 4 thereof. This request was verbally denied by Examiner Johnson, who asked that I ignore the sentence fragment that appeared to provide further information.

Due to the short time remaining for response, the undersigned further requested an interview in the present application, via a message on the Examiner's voice mail on Feb. 9, 2009. No response to this request was received. Applicants again reiterate this interview request and submits that under the circumstances, final rejection would be improper at this point.

Regarding the rejections under 35 U.S.C. §112

The Office rejects claims 1, 9, 16, 23, 29, 35, 41, 47 and 52 as failing to comply with the written description requirement. Applicant strenuously traverses this rejection, but has made amendments in an earnest attempt to reach common ground with the Examiner.

The Office submits that in claims 1, 9, 16, 23, 29 and 35 the language about termination of encryption activity is unclear. It is respectfully submitted that one of ordinary skill in the art upon review of the specification will have no doubts about what the claims are referring. However, in an effort to bring prosecution to a speedy conclusion, the claims have been amended

Application No.: 10/795,929

-15-

to indicate that the communication failure results in failure for the CA management system to cease providing and updating keys or encryption information to the CA encryption system (to paraphrase without intent of imposing limitations).

In claims 41, 47 and 52, regarding the term "alternate", while the word is not explicitly used in the specification, there is no legal requirement for such. At page 4, lines 8-11 the specification states that "The raw transport packets are passed along transport packet interface 1124 to the Cryptoperiod switch 1128, which switches periodically between even decrypt engine 1132 and odd decrypt engine 1136." A plain language reading of this language clearly indicates that the encryption systems alternate. However, the claims have been amended back to use "odd" and "even" language in an effort to assure that the Examiner is content with the language.

In the prior Office Action, the Office objected to use of the term decryption or encryption "keys". It is noted that these terms are directly supported by the claims as originally filed. Moreover, the specification uses the term "code words" which those skilled in the art of conditional access will appreciate that such terms are used interchangeably and synonymously in the art. The specification further refers to the DVB specification which teaches use of the alternating odd and even encryption scheme discussed.

With these explanations and amendments, the claims are submitted to more than fully comply with 35 U.S.C. §112.

Regarding the cited art in general

The Maillard reference of record describes a conditional access system that uses smart cards at the receiver for decryption functions. As is apparently acknowledged by the Examiner, Maillard does not disclose encrypting certain content using a default key in the event of a communication failure (see paragraph spanning pages 3 and 4). The Office seems to assert that Maillard discloses a default encryption mechanism, but the undersigned is unable to find any such disclosure.

The Bestler reference of record, as understood, describes use of session data packets that are alternately encrypted/decrypted with two different session keys (col.3, lines 1-6). When a new key (a third key) is provided by the headend, one of the old keys continues to work for a

Application No.: 10/795,929

-16-

time, while the other is rendered obsolete. New keys can thereby be introduced periodically as desired to enhance the system's security (col. 5, lines 19-22). Unauthorized users having only the obsolete key cannot decrypt the content once a polling cycle and key distribution cycle is complete (col. 5, lines 36-59). Although the current encryption key will continue to function when a polling cycle is missed (col. 5, lines 1-6), there is no disclosure for the continuation of encryption activity should a power fault or other system reset function occur and polling activity cannot be restarted due to a loss of communication with the content provider. A default key is discussed with reference to U.S. Patent no. 4,771,458. Reference to this patent indicates that the default key is used only for decryption of global data, not for addressed data "One of the global decryption keys is a permanent default key associated with the subscriber terminal to assure that communication with that terminal is possible despite a lack of knowledge of the terminal address or the other global decryption keys in its memory." (abstract) Thus, essentially, the default key is a key of last resort for communication of data between the headend and the subscriber terminal. There is no teaching or suggestion of use of this default key for communication of A/V content.

The Yonge reference discloses a default key, as noted at col 33, lines 7-17 the key is used to secure communication between multiple stations in a CSMA network (abstract). As such, this reference seems inapplicable to the present application since it fails to address any aspect of the problem being addressed.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-57 are rejected as being unpatentable over Maillard et al. (US Patent No. 6,466,671, hereinafter "Maillard") in view of Bestler et al. (US Patent No. 4,995,080, hereinafter "Bestler").

Regarding claims 1, 9, 16, 23, 29 and 35, these claims have been amended to provide clarification. Claim 1 as amended recites at least "encrypt certain audio/video content upon a communication failure between the conditional access encryption system and the conditional access management system in which said communication failure results in an inability for the conditional access management system to provide the encryption keys to the conditional access

Application No.: 10/795,929

-17-

encryption system, the default encryption key being distinct from keys supplied by and periodically changed by the conditional access management system". The other independent claims noted above contain similar features.

In order to establish *prima facie* obviousness, the Office Action must establish the presence of each claim feature of in the cited art and provide articulated reasoning with rational underpinning for the obviousness of the combination of claim features and their interrelationship. The Office Action admits that Maillard does not specifically disclose the encryption of certain content upon a communication failure between the conditional access system and the conditional access management system and looks to Bestler to remedy this lack. The Office Action seems to assert that these claim features are met by Bestler at col. 3, lines 1-6, col 5, lines 19-22, col. 5, lines 37-39 and col. 5, lines 60-63, however, they are not.

Bestler in the recited sections, discloses at most a failure of communication due to a polling error of some type that restricts the subscriber from receiving the latest update for the encryption for received content (col. 5, lines 1-6). There is no disclosure in Bestler for the special condition of what happens when the conditional access management system loses communication with the CA encryption system. The claims as amended explicitly address this. In Bestler, it appears that the prior encryption keys are used, but in real world applications, this does not always occur since the communication failure may result in loss of those keys by the encrypter. As a result, there are incidents wherein adult programming has been transmitted without the benefit of encryption. In accord with the claims, a dedicated set of default encryption parameters are used in such cases which would otherwise result in the audio/video content being distributed unencrypted. This prevents such material from reaching children which would otherwise not be prevented in Bestler.

Bestler, in the sections recited, discloses multiple encryption keys that are sent by a provider to a subscriber, and a process for continuing to decrypt provided content within the subscriber station by providing two different decryption keys that both will decrypt received content, then sending another key that will decrypt content while simultaneously disabling one of the two earlier keys. This is an efficient means for delivering additional decryption keys such that content continues to be decrypted by the most updated keys. However, this does not address

Application No.: 10/795,929

-18-

the condition that the recited claim elements address. The claims, however, have been amended to require that the default encryption key is stored in the memory and is distinct from the active encryption keys (or similar language). Hence, Bestler fails to disclose the default keys or other default encryption information as claimed.

As noted above, Yonge further fails to contribute to this combination in any meaningful way. Yonge only discloses a default key for communication between stations, but fails to fill the void in teachings that would lead one to the solution to the present problem. It is again noted that in DVB, stations do not communicate among themselves in the manner contemplated by Yonge's CDMA system.

The Office argues in certain instances that the combination proposed would be obvious because one would have been motivated to employ the teachings of Dasari in order to ensure efficient station-to-station dialog or QOS. However, Dasari is not used in the present rejection as best the undersigned can tell. Moreover, the Office provides no explanation as to how the proposed combination would accomplish efficient station-to-station dialog or QOS. There is no indication that the DVB communication method which Applicants have modified fail to provide efficient station-to-station dialog (in fact, no such dialog at all is provided in DVB encrypted cable television systems) and no nexus has been made to any improvement in QOS provided by the combination (note that QOS generally refers to the quality of data transmission – one could argue that imposing encryption actually inhibits QOS in that it inhibits reception by certain stations).

In other instances, the Office argues that the combination would permit a subscriber to self-authorize pay TV, but again the undersigned finds no nexus between the proposed motivation and the actual claimed combination. Applicants do not understand how the claims enable self authorization.

In order to establish *prima facie* obviousness, the Office is obligated to provide an articulated reasoning for making the proposed combination. The Office cannot simply find a collection of similar elements and assert the proposed combination to be obvious in the absence of such an articulated reasoning based upon evidence. The reasoning supplied is clearly inadequate since nothing addresses how one assures that there is always encryption on certain

Application No.: 10/795,929

-19-

content, and there is no explanation as to how the proposed combination would even accomplish that which is asserted to be motivated. In the case of Bestler, the prior encryption keys are apparently held over, but if Bestler's encryption engine re-initializes, there may be no encryption keys held over. In the claims, such situations would utilize the default encryption. No articulated reasoning has been provided that would account for a solution to this problem regardless of the proposed motiviation to combine. Maillard does not disclose encryption methods responsive to a communication failure, Bestler provides for certain communication failures, but not all, and Yonge only provides for a default encryption key used in inter-station communication. No viable articulated reasoning is provided that would put these pieces together in a manner that always assures some degree of protection by encryption. Hence *prima facie* obviousness has not been established.

The Office is further obligated to find all claim features arranged as claimed in order to establish *prima facie* obviousness. In view of the present amendments, it is submitted that the proposed rejections are inadequate. Reconsideration and allowance are respectfully requested.

In view of these amendments, all claims are submitted to be allowable for at least the reasons discussed above. Accordingly, reconsideration and allowance are respectfully requested.

Concluding Remarks

The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, it is submitted that further discussion is unnecessary. Applicant reserves the right to present further arguments at a later date for any of the rejected claims, but feels that the present arguments adequately address the rejections at hand.

Respectfully submitted,

/Jerry A. Miller 30779/

Jerry A. Miller
Registration No. 30,779

Dated: 2/10/2009

Application No.: 10/795,929

-20-

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337

Application No.: 10/795,929

-21-